REMARKS

Reconsideration of the rejections set forth in the Office action dated 01/16/2004 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-22 are pending

Claims 1-22 stand rejected.

Claims 4 and 16 are canceled.

Claims 1, 3, 5-9, 13, 15, and 17-21 were amended. Independent claims 1, and 13 were amended to include the limitation of canceled claims 4 and 16 respectively. Claim 20 was similarly amended. Claims 3, 5-9, 15, 17-19, and 21 were amended to be consistent with the amendments made to their respective parent claims.

I. *Drawings*

After receiving an office action for companion case 09/596,857 where the Examiner of that case noticed that figures 1A, 1B, and 1C were missing, the Applicant reviewed the instant case and has determined that the same figures are missing.

Applicant's current attorney of the instant case prepared an affidavit for the attorney of case 09/596,857. A copy of this affidavit is included herewith. Applicant's attorney for application 09/596,857 provided the following remarks (where the references have been updated for the instant application).

> ...After a review of our files, applicant believes that Figures 1A-1C were not sent with the application by the patent firm who wrote this application. Applicant includes herewith a proposed drawing correction that includes the missing figures. Figure 1B is described in the specification at page 12, lines 3-12. Figure 1C is described in the specification at page 12, lines 14-23. No new matter was added by the proposed Figures 1B and 1C as the text clearly describes what these proposed figures show. Thus, proposed Figure 1B and 1C simply conform to the specification.

Figure 1A is described starting at page 11, line 1 through page 12, line 3 --
and in the context established at page 9, line 23 through page 11, line 1.
Applicant's current attorney assigned the task of recreating Figure 1A to another
patent attorney, Mr. Daniel B. Curtis, reg: 39,159. According to Mr. Curtis'
affidavit filed herewith, Mr. Curtis read the specification, and prior to discussing
the issue with the inventors, used the specification and his own understanding of
the technology to conceptualize the cryptoserver architecture. Mr. Curtis reduced
his conceptualization to proposed Figure 1A and verified his conceptualization of
the system architecture with Inventor Smetters. Mr. Curtis is no more than skilled
in the art. Thus, no new matter was added by proposed Figure 1A because the
proposed figure is supported either directly or inherently, by the originally filed
specification, drawings, or claims as interpreted by one skilled in the art and
because proposed Figure 1A merely clarifies or completes the original disclosure.

As the disclosure for the instant application related to Figure 1A is slightly
different from the disclosure of Figure 1A in application 09/596,857, applicant's attorney
added identifying request handler threads as element 156, and added the reply 162.

Applicant's current attorney for the instant application (Mr. Curtis) also believes
that no new matter is added by Figures 1A, 1B, and 1C and respectfully requests that
Figures 1A, 1B, and 1C be approved and entered in the instant case.

I. Amendments to the specification

The amendments to the specification are not believed to add new matter, but were
made to correct typographical errors and to improve the clarity of the disclosure.

II. General Comments regarding the claimed invention

The currently claimed invention is directed towards a **cryptographic service**. The
cryptographic service is described at page 15, line 19 through page 16, line 4; page 19,
lines 13-19; and page 20, lines 17-22 (as well as the application as a whole).

To summarize, a cryptographic service provider operates a server. The server
provides cryptographic services to clients such that the client can off-load the
computational burden related to a cryptographic operation from the client computer to the
server that provides the service of performing the cryptographic operation. One example

of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a server that performs the requested cryptographic service for the client.

The server thus provides a cryptographic service to a client computer such that the client computer can off-load the computational burden due to cryptographic operations from the client computer to the cryptographic server.

The invention of currently amended claim 1 is directed to a networked server that provides a cryptographic service. The method includes the following steps.

(a)   identifying a client utilizing the network;

(b)   establishing a first key;

(c)   generating a tunnel on the network;

(d)   receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e)   performing the cryptographic service at the server for the client.

Thus, the claimed invention is directed to providing a cryptographic service from a networked server.

One observation, the Applicant points out that the Office Action did not specifically address claims 2, 7-12, 14, or 19.

IV. Rejections under 35 USC §103(a)

Original claims 1-22 stand rejected under 35 USC §103(a) as being unpatentable over McGarvey (6,643,774) in view of Kirby (5,898,784).

A prima facie case of obviousness is established when the Examiner provides one or more references that were available to the inventor and that teach a suggestion to

combine or modify the references the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

Applicant has amended the claims by replacing the term "work" with that of "cryptographic service". The cryptographic service is described at least at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22. Applicant believes that these claims are now patentable over the cited art.

With regards to McGarvey: McGarvey teaches techniques for allowing a server to use a client computer's (or user's) authority so that the server computer can access protected resources or perform protected services on behalf of the client (McGarvey column 2, lines 4-11; column 6, line 64 – column 7 line 16; and column 8, lines 52-56).

The problem addressed by McGarvey is how to allow a client computer to give a server the same access to protected data or services that the client has. It does this by delegating client authority to a server so that the server can access the protected data or services in place of the client. This delegation is accomplished by using a public key encryption system to establish trusted communication between a client, a server, and a private key system.

With regards to the limitations of Claims 4 and 16 that have been incorporated into their respective independent claims. Nothing in McGarvey teaches off-loading of a cryptographic service from a client to a server. McGarvey teaches techniques for sharing a client's ability to access protected data or service with a server so that the server can access the same protected data or service that the client could have accessed.

Nothing in McGarvey teaches to one skilled in the art a suggestion to modify McGarvey to include a networked server that provides cryptographic services (as that term is used in the application) to a client.

With regards to Kirby: Kirby teaches network tunneling and encryption techniques.

The problem addressed by Kerby is that of sending network packets through firewalls.

While Kirby recognizes the burden of encrypting and decrypting packets (Kirby: column 6, lines 25-40) Kirby suggests spreading the burden to multiple computers by terminating the virtual tunnels at the different computers.

Thus, nothing in Kirby teaches to one skilled in the art a suggestion to modify Kirby to include a networked server that provides cryptographic services to a client.

Nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to a networked server that provides cryptographic services to a client.

Thus, currently amended **claim 1** is believed to be patentable. Currently amended **claim 13** and currently amended **claim 20** are a program product claim and a system claim (respectively) that are comparable with currently amended claim 1 and so are also believed to be patentable for the same reasons.

Original claims 2 and 14 depend on and further limit their respective independent claims that are patentable and thus claims 2 and 14 are also patentable.

Currently amended claims 3 and 15 depend on and further limit their respective parent claims that are patentable and thus claims 3 and 15 are also patentable.

Currently amended claim 21 depends on and further limits patentable claim 3 and thus claim 21 is also patentable.

Claims 4 and 16 have been canceled and their limitations included in their respective independent claims.

Currently amended claims 5 and 17 depend on and further limit their respective independent claims that are patentable and thus claims 5 and 17 are patentable. Furthermore, nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to off-load modular exponentiation from a client to a cryptographic server.

Currently amended claims 6 and 18 depend on and further limit their respective independent claims that are patentable. Thus claims 6 and 18 are also patentable.

Original claim 22 depends on and further limits patentable claim 21 and thus claim 22 is also patentable.
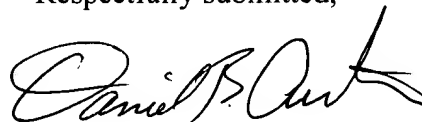
Currently amended claims 7-9 and 19; and original claims 10-12 depend on and further limit their respective parental claims that are patentable. Thus, claims 7-9, 10-12 and 19 are patentable.

No additional fee is believed to be required for this amendment. However, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,

Daniel B. Curtis
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com